UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,489	03/18/2004	Vincent J. Zimmer	42P18506	7634

7590 05/14/2008

Anthony H. Azure
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
VO, TED T	

ART UNIT	PAPER NUMBER
2191	

MAIL DATE	DELIVERY MODE
05/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,489	ZIMMER ET AL.	
	Examiner	Art Unit	
	TED T. VO	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,7-12,15-19 and 21-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-3,7-12,15-19 and 21-23* is/are allowed.

6)☒ Claim(s) *24-26* is/are rejected.

7)☒ Claim(s) *27* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 01/22/08.

Claims 1-3, 7-12, 15-19, 21-27 are pending in the application.

Response to Arguments

2. With regard to the arguments in the remarks filed on 01/22/08, the arguments have been considered but not persuasive.

Applicants' arguments merely are that *Garfinkel* fails to compute a compound hash value using information from a first and second virtual machine.

Applicants' argument is that *Garfinkel* teaches away from a second VM platform configuration include the second VM hash value because the teaching of Attestation is solely between a single VM and a single remote party. Applicants' argument is that *Garfinkel's* hashes are associated with single VM, and do not include a second VM hash value from a second VM platform configuration.

Examiner disagrees: TVMM is a trusted virtual machine monitoring. As it noted, Tara is such a tool that is based on a VMM to allow many virtual machines (VMs) to run independently and concurrently. Sec. 2.2, it discusses Attestation as VM identity, where hashes can be associated with VMs when loaded by the system boot loader of the TVMM. The Figure 1 is an exemplary view of the TVMM, that is based on one loaded VM, but it is clearly applied to

multiple VMs since the reference mentioned so. Since Each loaded VM it has a certification, in which the TVMM involves signing a hash of the VM for identifying. Thus each VM is associated with a hash, and put in the area "Hardware Platform" even it is views as single in the Figure 1. Therefore, with the ability of loading multiple VMs, the TVMM includes not only a second hash, but many hashes from all hashes of the VMs which are loaded. Therefore, each VM is associated with a hash and attestation.

Claim 24, it recites loading a first and a second VM, sharing a trusted hardware device between the first VM and second VM using a multiplexer. It is clearly being anticipated by the TVMM and in p. 194 ("The VMM can also multiplex the display and input devices"). The claim 24 recites computing and determining based on using the hashing values is merely for trusted computing that is the principle of the cited reference. Therefore, there is no way for *Garfinkel* to teach away from a second VM platform, as of Applicants' argument, when the TVMM is able to multiplex the VMs, and it has the ability to load multiple VMs and their devices. Furthermore, computation and recitations of "compound of Hashes" or a first VM and second VM in the claim cannot make the claimed invention novelty over a hash or a single VM as displayed over a VMM.

Applicants' argument fails discuss the patentability of these limitations in accordance to 1.111(b) and (c).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 24-26 are rejected under 35 U.S.C. 102(a) as being anticipated by Garfinkel et al., "Terra: A Virtual Machine-Based Platform for Trusted Computing", ACM, 2003.

Given the broadest reasonable interpretation of followed claims in light of the specification.

As per Claim 24: Garfinkel discloses,

A method, comprising:

loading a virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer (see p.194, left col., last paragraph, "allow many virtual machines (VMs) to run…": *plurality of virtual machines*. See Figure 1, TVMM: "VMM": i.e., TVMM is loaded in a hardware platform)*;* ***loading a first and a second virtual machine (VM) supported by the VMM*** (See sec. 2, p. 194, TERRA allows multiple VMs

running independently and concurrently, e.g., see left col., last paragraph of p. 194. See p. 196, left col., third paragraph);

and sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer (refer TVMM, T: trusted; see p. 194, right col., last paragraph, "multiplex");

receiving a request for a VMM service that is associated with the first VM, wherein the request comprises a challenger hash value (see p. 201, Secure Storage);

computing a current compound hash value based on a combination of the first VM platform configuration including the challenger hash value and the second VMplatform configuration including the second VM hash value (see p. 199, sec. 4.2); ***determining whether the current compound hash value is equal to the stored compound hash value; and executing the received request when the current compound hash value is equal to the stored compound hash value*** (See section 2, and see sec. 2.2).

As per Claim 25: Garfinkel discloses, *The method of claim 24 wherein the VMM is loaded from firmware, the firmware including instructions compliant with an Extensible Firmware Interface (EFI) specification* (See sec. 2.2, p.195-196, and p. 199, e.g., "firmware", "VM firmware", and see p.195, left col. Extensibility).

As per Claim 26: Garfinkel discloses, *The method of claim 1 wherein sharing the trusted hardware device comprises multiplexing a first request from the first VM and a second request from the second VM to the trusted hardware device using the VMM multiplexer* (See p. 194, right col., last paragraph, "multiplex", also see Figure 1).

Allowable Subject Matter

5. Claims 1-3, 7-12, 15-19, 21-23 are allowed.

Claims 27 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ted T. Vo whose telephone number is (571) 272-3706. The examiner can normally be reached on 8:00AM to 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wei Y. Zhen can be reached on (571) 272-3708.

The facsimile number for the organization where this application or proceeding is assigned is the Central Facsimile number 571-273-8300.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TTV
May 08, 2008

/Ted T. Vo/
Primary Examiner, Art Unit 2191